Remarks

Claims 1-6, 8-11, and 20-49 are in the application. Claims 1, 20, 27 and 33 are in independent form. Reconsideration is requested.

Claims 28, 36, 39-40 are objected to for various informalities. Claims 28, 36, 39-40 have been amended to correct the informalities identified by the Examiner.

Claim 35 is rejected under 35 USC 112, first paragraph, for lack of an enabling disclosure with regard to "software stored in the memory component to install or to run on the host computer is a Bluetooth application software." Claim 35 has been amended to delete the recited subject matter.

Claims 1, 35, and 40 are rejected under 35 USC 112, second paragraph, for indefiniteness. Claim 1 has been amended to correct the typographical error identified by the Examiner, and claims 35 and 40 have been amended to delete the trademark as suggested by the Examiner. Applicant requests that the rejection be withdrawn.

Claims 1-6, 8-9, and 20-40 stand rejected under 35 USC 103(a) for obviousness over US Publication No. 2003/0046447 by Kouperchaliak (hereafter Kouperchaliak) in view of Publication No. 2002/0145632 to Shmueli et al. (hereafter, Shmueli). Applicant responds as follows.

Claim 1 is amended to include the subject matter of former claim 3 and to emphasize a protected memory component where protected software is stored and in which the protected software is accessible only by the application launcher autorun software upon authentication of the application launcher autorun software. Amended claim 1 further recites that the software in the protected memory component is not viewable or accessible by the user, as described in the application at paragraph [0046]: "Private sections can be used to store installable or executables that cannot be viewed or accessed by the user."

With regard to claim 3 the Examiner states that

> However, Schmueli discloses in an analogous computer system the memory component includes a protected memory component and selected

> software is stored in the protected memory component and in which to the selected software is accessible by the autorun software upon authentication of the autorun software (paragraph [0011] "...the software on the portable device may provide an authentication routine instructing the host computing device to receive authentication indicia from the user via an interface on the host...determine if the authentication indicia received from the user matches authentication indicia stored on the portable device.., user must be authenticated...").
>
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method of the memory component includes a protected memory component and selected software is stored in the protected memory component and in which to the selected software is accessible by the autorun software upon authentication of the autorun software as taught by Shmueli into the method of automatic software/driver installation of a stored within the device as taught by Kouperchliak. The modification would be obvious because of one of ordinary skill in the art would be motivated to securely store the software in a protected area to provide privacy and security issues associated with computing on multiple computing devices on commercial and personal levels as suggested by Shmueli ((paragraph [0005]).

Kouperchaliak is directed to providing improved "plug & play" functionality of USB computer peripherals by allowing a USB peripheral to install the drivers needed to operate with a host computer. For example, Kouperchaliak describes a computer peripheral device such as a printer that has stored on it "device-related software (DRS)" (e.g., software drivers) that permit interaction between the printer and the computer. The printer checks whether device-related software (i.e., drivers) are already installed on the host computer and, if not, uploads the device-related software from mass storage device emulator to the computer for the proper installation and operation of the peripheral device by the computer.

Shmueli describes a portable device or "key" capable of interacting with a computing device to facilitate user interaction [Paragraph 002], the software on the portable device runs an authentication routine on host computing device via an interface to receive authentication indicia from the user [Paragraph 0011] to ensure that the user or holder of the key is authorized to use it on a host computer. The authentication routine provides a user authentication interface that requires a user to input a password, logon information, or biometric indicia from a

biometric reader associated with the host 12. The user provides the authentication indicia to the interface running on the host, the authentication routine determines if the user is authenticated and provides access to data on the key to the user accordingly.

Shmueli provides no teaching or suggestion of a protected software that is stored in the protected memory component and not being viewable or accessible by the user and only being accessible to be run by the application launcher software upon authentication of the application launcher software, as recited in the claim. Rather, Shmueli would lead one skilled in the art away from the combination of claimed features. In particular, Shmueli describes no protected memory component from which software is not viewable and is only accessible to be run by the autorun software. Shmeuli describes the key 10 as follows:

> "the software on the portable device may provide an authentication routine instructing the host computing device to receive authentication indicia from the user via an interface on the host computing device and determine if the authentication indicia received from the user matches authentication indicia stored on the portable device. As such, a user must be authenticated prior to using the portable device." Shmueli, Paragraph [0011]
>
> "Preferably, once an interaction between the key 10 and a host 12 is established, the memory 18 will emulate a file system on a memory device, such as a hard disk drive, accessible by the host 12 wherein at least certain aspects of the software 20 are capable of running or executing on the host 12." Shmueli, paragraph [0027].

Once he is authenticated by entry of his password the user of a Shmueli key 10 has access to view or copy any software stored on the key 10. Accordingly, Shmueli provides no indication of a protected memory component where software is not viewable. Shmueli further emphasizes the absence of any such protected memory area by relying upon user authentication or encryption for the protection of data stored on the key 10: "data may be accessed from the key 10 as necessary based on the keylet and the authentication" (Shmueli, paragraph [0039]) and "Preferably, this information is encrypted and protected in the user's key 10." (Shmueli, paragraph [0063]).

Schmueli describes a key 10 to which access is provided upon user authentication. In contrast, claim 1 recites authentication of the autorun software, not a user. Authentication of the autorun software is described in that application at paragraph [0051], for example. Authentication of the autorun software, rather than a user, allows the private memory component to provide software that is accessible to be by the autorun software while also being protected from being viewed or copied by a user. Schmueli provides no teaching or suggestion of protecting anything on a key 10 from an authenticated user and, therefore, provides no teaching or suggestion of the claimed subject matter.

Shmueli does not describe or even suggest a protected memory component with software that is only accessible to be run by the autorun software and further is not viewable. The Shmueli key does not provide "a security mechanism that can be incorporated to protect the software that is installable or executable from the memory component by the autorun firmware." (Present application, paragraph [0045].) Schmueli indicates that data on the key is further protected by encryption. It will be appreciated that protecting data or software on a key 10 of Schmueli is an indication that the key does not include a protected memory component that is not viewable or accessible by a user.

The inability to view software stored in a protected memory section according to the present invention, together with the software in the protected memory component only being accessible to be run by the autorun software, provide a secure manner of distributing the software without risk of it being improperly copied or otherwise accessed. In contrast, the apparent user accessibility to software on key 10 once a user has been authorized exposes the software on key 10 to improper viewing, copying, etc. Applicant submits, therefore, that claim 1 is patentably distinct from the cited references.

Independent claim 20 stands rejected for the reasons set forth above with respect to the rejection of claim 3. Applicant notes, however, that claim 20 recites "a protected memory component where the selected software is stored component so as not to be viewable." Claim 3 did not previously recite such a

feature, which is not recited in amended claim 1, as described above. The rejection of claim 20 does not address this feature in the cited art. Applicant submits, therefore, that the rejection of claim 20 was improper and should be withdrawn for failure to identify in the prior art each and every feature recited in the claim. Moreover, applicant submits that claim 20 is patentably distinct from the cited art for the reasons set forth above with regard to claim 1.

Independent claim 27 recites a user operable manual switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device.

Shmueli describes a portable "key" with an authentication system that does not relate to such a switch. Kouperchaliak includes an automated, non-manual "function switch 36" that automatically switches a peripheral device between a device driver installation mode and a normal peripheral function mode according to whether the device driver is installed on a host computer. Kouperchaliak provides no teaching or suggestion related to a user-operable switch that allows a user to select from among plural operating states that include a first state in which the autorun software is operable and a second state in which the autorun software is not operable so that the integrated circuit flash drive memory device functions as a conventional integrated circuit flash drive memory device. Rather than being mere design choice, the fully-automated operation of the "function switch" of Kouperchaliak relates directly to the one-time installation of device drivers.

The Examiner cites paragraph [0037] of Kouperchaliak as disclosing the user operable manual switch recited in the claim. In that passage, Kouperchaliak recites "one or more configuration files that allow a peripheral device to be configured in different ways." Applicant notes that the configuration files of Kouperchaliak relate to configuration of a peripheral device, not the operation of the integrated circuit flash drive memory device recited in the claim. Moreover,

Kouperchaliak provides no teaching or description of the autorun software recited in the claim, and Shmueli describes a key 10 with that "is preferably configured for autorun capability, which ... will allow a start-up application stored on the key 10 to start executing when the key 10 is plugged in to the USB port of the host 12. (Shmueli, paragraph [0028].) Nothing in either of the cited references teaches or suggests any user operable manual switch, much less such a switch that turns autorun software off or on. Instead, applicant submits that Shmueli would lead one skilled in the art away from such a switch by emphasizing that the autorun capability is started upon plugging the key 10 into a host computer. Applicant submits, therefore, that claim 27 is patentably distinct from the cited references.

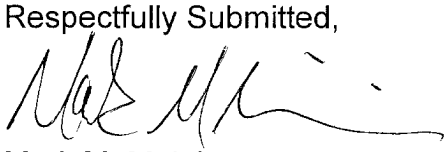
Independent claim 33 recites an integrated circuit wireless device connectable to a host computing device and includes a wireless component for enabling the host computing device wireless connectivity with the wireless component. A memory component includes a protected memory component where the wireless application software is stored so as not to be viewable and is accessible only by the autorun software during installation or running of the wireless application software, thereby providing copy protection of the wireless application software. Applicant submits that the new independent claim 33 is distinct from the cited references for reasons set forth above in regard to independent claims 1, 20, and 27.

Applicant submits that dependent claims 2, 4-6, 8-9, 21-26, 28-32, and 34-40 are patentably distinct as depending from their respective base claims.

Applicant believes the application is in condition for allowance and respectfully requests the same.

IPSOLON LLP
111 SW COLUMBIA #710
PORTLAND, OREGON 97201
TEL. (503) 249-7066
FAX (503) 249-7068

Respectfully Submitted,



Mark M. Meininger
Registration No. 32,428